

#2

JC925 U.S. PTO  
09/685859

10/11/00

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-020718

(43)Date of publication of application : 21.01.2000

(51)Int.Cl.

G06T 7/00

G06F 19/00

(21)Application number : 10-180935 (71)Applicant : FUJITSU LTD

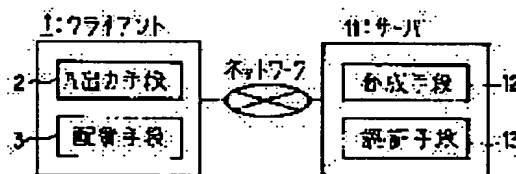
(22)Date of filing : 26.06.1998 (72)Inventor : SATAKE SHUICHI

## (54) CERTIFICATION SYSTEM AND RECORDING MEDIUM

## (57)Abstract:

PROBLEM TO BE SOLVED: To prevent a seal from being illegally used and to detect modification of a document after checking the seal with respect to a certification device for arranging a seal image on a document by preparing a keyword based on disclosed information and document information, integrating the keyword in a bit map, arranging a seal image obtained by compositing the seal image and the bit map on a document, and extracting the arranged seal image from the received image to collate it.

SOLUTION: The certification system is provided with a 1st composite means for preparing a keyword from the document information of a document on which information related to a user and a seal image are to be arranged and incorporating the keyword in a bit map, a 2nd composite means 12 for compositing the integrated pattern with the seal image and a means 3 for arranging the seal image obtained after synthesis by the means 12 on a prescribed position of the document.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision  
of rejection][Kind of final disposal of application  
other than the examiner's decision of  
rejection or application converted  
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-20718

(P2000-20718A)

(43) 公開日 平成12年1月21日 (2000.1.21)

(51) Int.Cl.

識別記号

F I

テーム (参考)

G 0 6 T 7/00

G 0 6 F 15/62

4 5 5

5 B 0 4 3

G 0 6 F 19/00

15/30

H

5 B 0 5 5

審査請求 未請求 請求項の数 6 O L (全 11 頁)

(21) 出願番号

特願平10-180935

(22) 出願日

平成10年6月26日 (1998.6.26)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 佐竹 修一

富山県婦負郡八尾町保内二丁目2番1 株  
式会社富山富士通内

(74) 代理人 100089141

弁理士 岡田 守弘

Fターム (参考) 5B043 AA07 AA10 BA09 EA01 FA07

HA02

5B055 HA12 HB05 JJ00

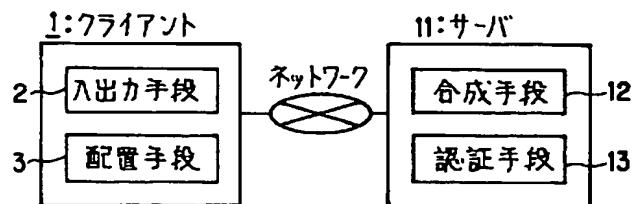
(54) 【発明の名称】 認証システムおよび記録媒体

(57) 【要約】

【課題】 本発明は、文書に印鑑イメージを配置する認証装置に関し、秘密情報、公開情報および文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置および受信文書から配置された印鑑イメージを取り出して照合し、印鑑の不正使用を防止すると共に検印後の文書の改変を検出することを目的とする。

【解決手段】 利用者に関する情報および印鑑イメージを配置しようとする文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第1の合成手段と、組み込んだパターンと印鑑イメージを合成する第2の合成手段と、第2の合成手段によって合成した後の印鑑イメージを文書中の所定位置に配置する手段とを備えるように構成する。

本発明のシステム構成図



## 【特許請求の範囲】

【請求項 1】文書に印鑑イメージを配置する認証装置において、

利用者に関する情報および印鑑イメージを配置しようとする文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第 1 の合成手段と、上記組み込んだパターンと印鑑イメージを合成する第 2 の合成手段と、

上記第 2 の合成手段によって合成した後の印鑑イメージを文書中の所定位置に配置する手段とを備えたことを特徴とする認証システム。

【請求項 2】受信した文書中に配置された印鑑イメージの認証を行う認証装置において、

利用者に関する情報および受信した文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第 1 の合成手段と、

上記組み込んだパターンと印鑑イメージを合成する第 2 の合成手段と、

上記第 2 の合成手段によって合成した後の印鑑イメージと、受信した文書中から取り出した印鑑イメージとを比較して一致したときに真、不一致のときに偽と判別する手段とを備えたことを特徴とする認証システム。

【請求項 3】上記利用者に関する情報として、利用者のパスワードを含む秘密情報および利用者の名前を含む公開情報としたことを特徴とする請求項 1 あるいは請求項 2 記載の認証システム。

【請求項 4】上記文書の文書情報として、印鑑イメージを配置しようとする文書中の文字数を含む文書情報としたことを特徴とする請求項 1 から請求項 3 のいずれかに記載の認証システム。

【請求項 5】利用者に関する情報および印鑑イメージを配置しようとする文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第 1 の合成手段と、

上記組み込んだパターンと印鑑イメージを合成する第 2 の合成手段と、

上記第 2 の合成手段によって合成した後の印鑑イメージを文書中の所定位置に配置する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項 6】受信した文書中に配置された印鑑イメージの認証を行う認証装置において、

利用者に関する情報および受信した文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第 1 の合成手段と、

上記組み込んだパターンと印鑑イメージを合成する第 2 の合成手段と、

上記第 2 の合成手段によって合成した後の印鑑イメージと、受信した文書中から取り出した印鑑イメージとを比較して一致したときに真、不一致のときに偽と判別する手段として機能させるプログラムを記録したコンピュー

タ読取可能な記録媒体。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、文書に印鑑イメージを配置する認証装置および記録媒体に関するものである。

【0002】

【従来の技術】複数のコンピュータをネットワークを介して接続したシステムにおいて、決裁業務をグループウェアを利用して電子的に行う電子決裁システムが広く知られている。

【0003】従来、電子決裁システムでは、印鑑データをイメージデータの形で予めサーバに保有し、パスワードの入力により特定文書の特定位置に印鑑イメージを配置し、決裁がされた旨を表すようにしていた。

【0004】

【発明が解決しようとする課題】しかし、入力時にパスワードで認証する方法を採用していたため、検印文書毎に印鑑イメージを変えることが難しく、どの電子媒体においても同一の印鑑イメージが付加されてしまい、印鑑イメージの偽造や盗用されてしまう可能性があるという問題があった。

【0005】更に、検印後に文書を変更された場合の確認ができないという問題もあった。本発明は、これらの問題を解決するため、秘密情報、公開情報および文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置および受信文書から配置された印鑑イメージを取り出して照合し、印鑑の不正使用を防止すると共に検印後の文書の改変を検出することを目的としている。

【0006】

【課題を解決するための手段】図 1 を参照して課題を解決するための手段を説明する。図 1 において、クライアント 1 は、ネットワークを介したサーバ 11 と相互に通信して各種業務処理を行うものであって、ここでは、入出力手段 2、および配置手段 3 から構成されるものである。

【0007】入出力手段 2 は、パスワードや社員番号などの各種情報を入力したり、操作指示したり、結果を表示したりなどするものである。配置手段 3 は、印鑑イメージを文書中の所定位置に配置するものである。

【0008】サーバ 11 は、ネットワークを介してクライアント 1 からの要求を受信したり、要求に対する応答を返信したりなどするものであって、ここでは、合成手段 12、認証手段 13 から構成されるものである。尚、合成手段 12 および認証手段 13 をサーバ 11 に設けたが、クライアント 1 内に設けるようにしてもよい。

【0009】合成手段 12 は、利用者に関する情報（秘密情報および公開情報）および文書情報からキーワード

を作成し、このキーワードをビットマップに組み込んだりするものである。

【0010】認証手段13は、文書中から取り出した印鑑イメージと、利用者に関する情報および文書から取り出した文書情報をもとにキーワードを作成しこのキーワードをビットマップに組み込んだ印鑑イメージとを、照合して認証するものである。

【0011】次に、動作を説明する。合成手段12を構成する第1の合成手段が利用者に関する情報および文書の文書情報からキーワードを作成してこのキーワードをビットマップに組み込み、合成手段12を構成する第2の合成手段が組み込んだパターンと印鑑イメージとを合成し、配置手段3が合成した後の印鑑イメージを文書中の所定位置に配置するようにしている。

【0012】また、合成手段12を構成する第1の合成手段が利用者に関する情報および受信した文書の文書情報からキーワードを作成してこのキーワードをビットマップに組み込み、合成手段12を構成する第2の合成手段が組み込んだパターンと印鑑イメージとを合成し、認証手段13が合成した後の印鑑イメージと、受信した文書中から取り出した印鑑イメージとを比較して一致したときに真、不一致のときに偽と判別するようにしている。

【0013】これらの際に、利用者に関する情報として、利用者のパスワードを含む秘密情報および利用者の名前を含む公開情報としている。また、文書の文書情報として、印鑑イメージを配置しようとする文書中の特定文字の文字数を含む文書情報としている。

【0014】従って、パスワードを含む秘密情報、利用者の氏名を含む公開情報および文書の文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置したり、受信文書から配置された印鑑イメージを取り出して照合したりすることにより、印鑑の不正使用を防止すると共に検印後の文書の改変を検出することが可能となる。

【0015】

【発明の実施の形態】次に、図2から図12を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0016】図2は、本発明の概念説明図(その1)を示す。図2の(a)は、ビットマップ(識別データ)の作成手順例を示す。図2の(a-1)は、秘密情報(パスワードなど)、公開情報(検印日付けなど)および文書情報をもとにキーワードを合成する様子を示す。ここで、秘密情報は、利用者個人のみが知っているパスワードなどの秘密情報である。公開情報は、利用者の公開している情報であって、下記のものがある。

【0017】

- ・社員番号
- ・名前

・役職

・その他

また、文書の文書情報としては、印鑑イメージを配置しようとする文書(受信した文書を含む)の文書に関する情報であって、例えば下記のようなものである。

【0018】

- ・文書内文字数(総文字数)
- ・ひらがな文字数
- ・カタカナ文字数
- ・空白文字数
- ・数字文字数
- ・特定文字数(複数可)
- ・その他

これら秘密情報、公開情報および文書情報をもとに、キーワードを作成する(図12を用いて後述する)。

【0019】図2の(a-2)は、①キーワードと②ビットマップを合成し、キーワード埋め込み後の③ビットマップを生成する様子を示す。図2の(a-2)において、①キーワードは、図2の(a-1)で合成したキーワードである。

【0020】②ビットマップは、キーワード埋め込み前の黒ベタのビットマップである。③ビットマップは、キーワード埋め込み後のビットマップである。この③ビットマップは、ここでは、①キーワードと、黒ベタの②ビットマップとをドット対応でAND合成したものである。ここでは、黒を“1”とし、以下も同様である。尚、白を“1”とした場合には、ORとなる。

【0021】図2の(b)は、検印用印鑑イメージの作成手順例を示す。図2の(b)において、④検印者登録印鑑イメージは、検印者の生の登録した印鑑イメージである。

【0022】③ビットマップは、図2の(a-2)のキーワード埋め込み後のビットマップである。⑤印鑑イメージは、④印鑑イメージと、③ビットマップとをAND合成した後の印鑑イメージであって、文書中の所定位置に配置しようとする印鑑イメージである。この印鑑イメージ⑤は、キーワードを黒ベタのビットマップに埋め込み(ビット対応でAND演算して埋め込み)、更に④印鑑イメージでAND合成したいわば当該印鑑イメージで打ち抜いた形の印鑑イメージであり、復元は不可能な一方通行の合成を行ったものである。

【0023】以上のようにして、秘密情報(パスワードなど)、公開情報(利用者の氏名、役職など)および文書情報(文書内の総文字数、ひらがな総文字数など)をもとにキーワードを合成し、キーワードとビットマップ(例えば黒ベタのビットマップ)を合成したキーワードを埋め込んだ③ビットマップを生成し、更に、生の④印鑑イメージでAND演算していわば当該④印鑑イメージで打ち抜いて⑤印鑑イメージを生成し、この⑤印鑑イメージを文書中の所定位置に配置して電子捺印することに

より、秘密情報、公開情報および文書情報を非可逆的な合成を行って文書中に配置して印鑑イメージの盗用や文書の改変を防止することが可能となる。

【0024】図3は、本発明の概念説明図(その2)を示す。これは、図2の②ビットマップが黒ベタであるのに対して、白ベタにした場合のものである。図3の

(a)は、ビットマップ(識別データ)の作成手順例を示す。

【0025】図2の(a-1)は、秘密情報(パスワードなど)、公開情報(検印日付けなど)および文書情報をもとにキーワードを合成する様子を示す。ここで、秘密情報は、利用者個人のみが知っているパスワードなどの秘密情報である。公開情報は、利用者の公開している情報であって、下記のものがある。

【0026】

- ・社員番号
- ・名前
- ・役職
- ・その他

また、文書の文書情報としては、印鑑イメージを配置しようとする文書(あるいは受信した文書)の文書に関する情報であって、例えば下記のようなものである。

【0027】

- ・文書内文字数(総文字数)
- ・ひらがな文字数
- ・カタカナ文字数
- ・空白文字数
- ・数字文字数
- ・特定文字数(複数可)
- ・その他

これら秘密情報、公開情報および文書情報をもとに、キーワードを作成する(図12を用いて後述する)。

【0028】図3の(a-2)は、①キーワードと②ビットマップを合成し、キーワード埋め込み後の③ビットマップを生成する様子を示す。図2の(a-2)において、①キーワードは、図2の(a-1)で合成したキーワードである。

【0029】②ビットマップは、キーワード埋め込み前の白ベタのビットマップである。③ビットマップは、キーワード埋め込み後のビットマップである。この③ビットマップは、ここでは、①キーワードと、白ベタの②ビットマップとをドット対応でOR合成したものである。

【0030】図3の(b)は、検印用印鑑イメージの作成手順例を示す。図3の(b)において、④検印者登録印鑑イメージは、検印者の生の登録した印鑑イメージである。

【0031】③ビットマップは、図3の(a-2)のキーワード埋め込み後のビットマップである。⑤印鑑イメージは、④印鑑イメージと、③ビットマップとを合成した後の印鑑イメージであって、ここでは、④印鑑イメー

ジの外枠で③ビットマップを打ち抜き(マスクして)その内部はビット対応でOR合成したものであり、文書中の所定位置に配置しようとする印鑑イメージである。この印鑑イメージ⑤は、キーワードを白ベタのビットマップに埋め込み(ビット対応でOR演算して埋め込み)、更に④印鑑イメージでOR合成した印鑑イメージであり、復元は不可能な一方通行の合成を行ったものである。

【0032】以上のようにして、秘密情報(パスワードなど)、公開情報(利用者の氏名、役職など)および文書情報(文書内の総文字数、ひらがな総文字数など)をもとにキーワードを合成し、キーワードとビットマップ(白ベタのビットマップ)を合成したキーワードを埋め込んだ③ビットマップを生成し、更に、生の④印鑑イメージでOR演算および印鑑イメージの外枠で打ち抜いて⑤印鑑イメージを生成し、この⑤印鑑イメージを文書中の所定位置に配置して電子捺印することにより、秘密情報、公開情報および文書情報を非可逆的な合成を行って文書中に配置して印鑑イメージの盗用や文書の改変を防止することが可能となる。

【0033】次に、図4のフローチャートに示す順番に従い、既述した図1から図3の構成および概念を使用した本願発明の実施例について詳細に説明する。図4は、本発明の動作説明フローチャート(その1)を示す。

【0034】図4において、S1は、社員番号を登録する。S2は、暗証番号を登録する。S3は、検印用文書情報を登録する。これらS1からS3は、例えば後述する図5の(a)の画面をクライアント1の表示装置上に表示し、利用者が自身の社員番号「1234567890」、暗証番号「\*\*\*\*\*」(\*は任意の英数字、記号などを表す)、検印用文書情報をキー入力あるいは画面上から選択入力する。ここで、検印用文書情報は、図5の(a)の画面上に示すように、文書内文字数、ひらがな文字数、かたかな文字数、空白文字数、数字文字数などの項目中から選択入力、および特定文字の文字数(複数可)を選択したときは更に右下領域にその特定文字をキー入力し、検印対象の文書中から自動採取すべき文書情報を指定する。ここで、社員番号は利用者の公開情報であり、暗証番号は利用者の秘密情報であり、検印用文書情報が文書情報である。

【0035】S4は、名前を登録する。S5は、役職を登録する。S6は、印鑑形状を登録する。

【0036】S7は、印鑑サイズを登録する。これらS4からS7は、例えば後述する図5の(b)の画面をクライアント1の表示装置上に表示し、利用者が自身の名前「富士」、役職「開発課長」、印鑑形状「丸(日付け有)」、印鑑サイズ「12mm」をキー入力し、サーバ11に登録する。

【0037】S8は、登録印鑑イメージを作成する。これは、印鑑イメージについては、スキャナーを用いて予

めあるいは同時に読み込んで作成し、サーバ11に登録する。ここで、印鑑イメージがドロウ（ベクトル）情報である場合には、スキャナは不要である。利用者のサインなどを使うときにスキャナを用いて電子化した印鑑イメージにする。

【0038】以上によって、利用者は図5の（a）、（b）の画面上から公開情報（利用者の社員番号、名前、役職など）、秘密情報（暗証番号など）、および印鑑イメージとその情報（印鑑形状、印鑑サイズなど）を入力してここでは、サーバ11に登録する。

【0039】図5は、本発明の画面例を示す。図5の（a）は、検印者情報の設定の画面例を示す。この画面では、図示の下記の情報を入力あるいは選択するものである。

【0040】

- ・社員番号：例えば「1234567890」を入力
- ・暗証番号：例えば「\*\*\*\*\*」を入力
- ・検印用文書情報（☐をチェックして選択）

☐文書内文書数：

☐ひらがな文字数

☐かたかな文字数

☐空白文字数

☐数字文字数

☐特定文字の文字数（複数可）：この場合には、右下ウィンドウに特定文字をキー入力

以上の項目を入力あるいは選択し、登録ボタンを押下すると、クライアント11からネットワークを介してサーバ11に登録されることとなる。

【0041】図5の（b）は、印鑑イメージ登録の画面例を示す。この画面では、図示の下記の情報を入力あるいは選択入力するものである。

- ・名前：例えば「富士」を入力
- ・役職：例えば「開発課長」を入力
- ・印鑑形状：例えば「丸（日付け有）」をプルダウンメニューから選択
- ・印鑑サイズ：例えば「12mm」を増減ボタンを押下して設定入力
- ・印鑑イメージ：上記データから検索されたイメージを表示

以上の項目を入力あるいは選択し、登録ボタンを押下すると、クライアント11からネットワークを介してサーバ11に登録されることとなる。

【0042】図6は、本発明の動作説明フローチャート（その2）を示す。図6において、S11は、印鑑設置領域の選択を行う。これは、利用者が後述する図7の（a）の表示装置の画面上に表示した文書中の検印欄を、印鑑設置領域として選択する。

【0043】S12は、社員番号を通知する。S13は、暗証番号を通知する。S14は、検印文書を送付する。これらS11からS14は、利用者がクライアント

1の表示装置の後述する図7の（a）の画面上で印鑑設置領域を文書中の検印欄を指定、社員番号を入力、暗証番号を入力した後、検印文書と一緒にこれら情報をネットワークを介してサーバ11に送付する。

【0044】S15は、登録印鑑イメージを検索する。これは、サーバ11でS12の社員番号、S13の暗証番号をもとに当該利用者の登録印鑑イメージを検索して取り出す。

【0045】S16は、キーワードを作成する。これは、既述した図2の（a）、図3の（a）で説明したように、秘密情報（暗証番号など）、公開情報（社員番号、名前、役職など）および文書情報をもとにキーワードを作成する。

【0046】S17は、ビットマップを作成する。これは、S16で作成したキーワードをビットマップに組み込んで作成する（図2の（a-2）、図3の（a-2）参照）。

【0047】S18は、検印用印鑑イメージを作成する。これは、S17で作成したキーワードを埋め込んだビットマップと、印鑑イメージとを合成して検印用印鑑イメージを作成する（既述した図2の（b）、図3の（b）参照）。

【0048】S19は、検印用印鑑イメージを通知する。これは、サーバ11がS18で作成した検印用印鑑イメージをネットワークを介してクライアント1に通知する。S20は、検印用印鑑イメージの文書内埋め込みを行う。これは、S19でサーバ11からクライアント1が受信した検印用印鑑イメージを、後述する例えば図7の（b）のS11で選択された検印の欄に配置する（埋め込む）。

【0049】以上によって、クライアント1が検印対象の文書中から検印領域の選択、公開情報（社員番号など）、秘密情報（暗証番号など）および文書情報をサーバ11に送信し、サーバ11がこれら情報をもとにキーワードを作成して印鑑イメージと合成して非可逆的な検印用印鑑イメージを生成し、クライアントに送信し、クライアント1が検印対象の文書中に配置し（埋め込み）、一連の検印処理を終了する。これにより、利用者の公開情報、秘密情報、文書情報および印鑑イメージを非可逆的に合成した検印用印鑑イメージを作成して文書中に配置することで、盗用されることなく、検印後に文書が改変されても検出できる検印用印鑑イメージで文書に検印することが可能となる。

【0050】図7は、本発明の画面例を示す。図7の（a）は、文書に検印するときの検印実行画面の例を示す。図7の（a）において、左下の検印の欄は、文書中の検印する領域として選択する領域である。

【0051】右側の検印の実行の画面は、文書の上に表示された別ウィンドウであって、ここでは、検印の実行に必要な図示の下記の情報を入力する画面である。

・社員番号：

・暗証番号：

以上のように、検印領域の選択（検印欄を選択）、社員番号、暗証番号を入力して確認ボタンを押下すると、自動的にクライアント1からネットワークを介してサーバ11に送信されることとなる（既述した図6のS1からS14）。

【0052】図7の（b）は、文書に検印するときの検印実行通知画面の例を示す。ここで、左下の検印の欄には、検印用印鑑イメージが配置されている（埋め込まれている）（既述した図6の20）。

【0053】以上のように、選択した検印の欄に、サーバ11から送られてきた検印用印鑑イメージを配置することで、利用者の公開情報、秘密情報、文書情報、および印鑑イメージから合成した非可逆的な検印用印鑑イメージを文書中の検印欄に自動的に配置し、検印を行うことが可能となる。

【0054】図8は、本発明の動作説明フローチャート（その3）を示す。これは、既述したキーワードをビットマップに組み込んで作成するときの詳細フローチャートである。

【0055】図8において、S31は、ビットマップを作成する。ここでは、例えば既述した図2の（a-2）の黒ベタの②ビットマップ、あるいは図3の（a-2）の白ベタの②ビットマップを作成する。

【0056】S32は、キーワードから乱数発生用関数を作成する。これは、例えば既述した図2の（a-1）で作成したキーワードから乱数発生用関数を作成する（図12参照）。

【0057】S33は、ピクセルデータの書換えを行う。これは、S32で作成した乱数発生用関数をもとに、ピクセル単位にS31で作成したビットマップの書換えを行い、キーワードを埋め込んだビットマップを作成する。

【0058】以上によって、ビットマップについて、キーワードから作成した乱数をもとにピクセル単位に書換えを行い、キーワードを埋め込んだビットマップを自動作成することが可能となる。

【0059】図9は、本発明の動作説明フローチャート（その4）を示す。図9において、S41は、確認検印の指定を行う。これは、例えば後述する図10の（a）の文書中の検印欄の印鑑イメージの検印の確認の指定を行う。

【0060】S42は、社員番号を通知する。S43は、検印文書情報を通知する。S44は、検印用印鑑イメージを通知する。

【0061】S45は、検印文書を送付する。これらS41からS45は、クライアント1の表示装置の画面上で利用者が検印対象の文書を表示し、確認する検印（印鑑イメージ）を指定し、社員番号、検印文書情報、検印

用印鑑イメージ、検印文書をサーバ11に送信する。

【0062】S46は、キーワードを作成する。これは、サーバ11が、利用者の公開情報（社員番号など）、秘密情報（暗証番号など）、文書情報（文書内の総文字数など）からキーワードを作成する。

【0063】S47は、登録印鑑イメージを検索する。これは、社員番号と暗証番号をもとに該当する生の印鑑イメージを検索して取り出す。S48は、確認印鑑イメージを作成する。これは、S47で取り出した利用者の印鑑イメージ、およびS46で作成したキーワードをもとに既述したようにして検印用印鑑イメージを作成する。

【0064】S49は、印鑑イメージを比較する。これは、S48で作成した検印用印鑑イメージと、S44でクライアント1から通知を受けた検印対象の文書から取り出した印鑑イメージとをビット対応で一致するか否かを比較する。一致する場合には、検印対象の文書から取り出した印鑑イメージが真正のものと判定し、不一致の場合には、偽のものと判定する。

【0065】S50は、比較結果を通知する。これにより、クライアント1は、サーバ11からS49で比較した結果（真正、偽）の受け取り、文書中の印鑑イメージが真正か（後述する図10の（b）参照）、偽か（後述する図10の（c）参照）を認識できることとなる。

【0066】以上によって、検印対象の文書中から取り出した印鑑イメージについて、当該文書の文書情報、公開情報（利用者の社員番号など）、秘密情報（暗証番号など）をもとにキーワードを作成し、当該キーワードと生の印鑑イメージとから作成した検印用印鑑イメージを比較した一致したときに真正、不一致のときに偽と判定することにより、印鑑イメージの盗用や検印後の文書の改変を検出することが可能となる。

【0067】図10は、本発明の画面例を示す。図10の（a）は、検印確認実行画面の例を示す。これは、検印対象の文書中から検印する対象の領域として、ここでは、検印の欄を選択した指定した状態を示す。右側のウィンドウ上に選択した領域の検印を確認するメッセージが表示されているので、確認ボタンを押下すると検印処理が開示される。

【0068】図10の（b）は、検印確認画面（正当）の例を示す。これは、検印対象の文書中の指定した検印欄の印鑑イメージについて、既述した図9のS41からS50による処理によって、クライアント1の表示装置の画面上に表示された、正当の場合の検印確認画面である。ここでは、「選択した領域の検印が正当（真正）です」というメッセージを表示し、検印欄の印鑑イメージが改変されていなく、かつ、検印対象の文書が改変されていない旨を表示したものである。

【0069】図10の（c）は、検印確認画面（不当）の例を示す。これは、検印対象の文書中の指定した検印



欄の印鑑イメージについて、既述した図9のS41からS50による処理によって、クライアント1の表示装置の画面上に表示された、不当の場合の検印確認画面である。ここでは、「選択した領域の検印が不当（偽）です、直ちに担当部署に連絡して下さい」というメッセージを表示し、検印欄の印鑑イメージが改変、あるいは検印対象の文書が改変されている旨を表示したものである。

【0070】図11は、本発明の印鑑イメージテーブル例を示す。これは、サーバ11に保存する印鑑イメージテーブルの例であって、ここでは、図示の下記の項目を対応づけて登録したものである。

【0071】

- ・社員番号：
- ・暗証番号：
- ・イメージファイル：印鑑イメージ
- ・属性：印鑑イメージの属性（印鑑サイズ、印鑑形状など）

図12は、本発明のキーワード組み込み説明図を示す。これは、既述した公開情報、文書情報、秘密情報をもとにキーワードを生成した後、乱数を生成するときの具体例である（図8参照）。

【0072】図12の（a）、（b）は、パレットデータおよびピクセルデータの例をそれぞれ示す。これは、16色ないし256色のビットマップは、通常、パレット部とピクセルデータ部を持ち、パレット部は色の数、ピクセルデータ部はビットマップを構成するドットの数分存在してその値は使用するパレットのインデックス番号である。ここで、パレットデータ内にあるデータはRGB情報であり、ピクセルデータ内にあるデータはビットマップを構成するドットが使用しているパレットの番号である。このため、パレット0が黒である場合、黒ベタのビットマップのピクセルデータの値は、全て0となる。

【0073】図12の（c）は、パスワード（秘密情報）、検印日付け（公開情報）、文書内文字数（文書情報）の例を示す。ここでは、図示の下記の値を持つとする。

- ・パスワード（秘密情報）：1234
- ・検印日付け（公開情報）：980303
- ・文書内文字数（文書情報）：980302

図12の（d）は、キーワードの例を示す。これは、図12の（c）のパスワード、検印日付け、文書内文字数を順に並べて図示の下記の数字列をキーワードとして生成する。

【0074】

- ・キーワード：1234980303980302

図12の（e）は、キーワードを4分割し、定数を作成する。これは、図12の（d）のキーワードを先頭から4つ飛び、第2番目から4つ飛び、第3番目から4つ飛

び、第4番目から4つ飛びに図示の下記の定数1から定数4を作成する。

【0075】

- ・定数1：1900
- ・定数2：2833
- ・定数3：3090
- ・定数4：4382

図12の（f）は、3次曲線を作成する。これは、図12の（e）の定数1、2、3、4をXの関数の定数の3次、2次、1次、定数に代入して図示の下記の3次曲線を作成する。

【0076】

$$Y = 1900X^3 + 2833X^2 + 3090X + 4382$$

図12の（g）は、図12の（f）の3次曲線の値を255（256個目のパレットは背景の白に残しておく）で割った余りを求めて乱数を生成する様子を示す。これは、図12の（f）の式のXにピクセルデータのインデックス値を代入して得られたYの値をパレット数（ここでは256としている）で割った余りをピクセルデータに格納すれば、ビットマップにキーワードを組み込むことが可能となる。

【0077】尚、完成したビットマップが使用するパレットの色が全て黒ならば、組み込み後も黒ベタのビットマップとなる。また、実際に使用する関数は以下になるため、キーワードを組み込んだビットマップからキーワードを分離することはできない。

$$Y = (1900X^3 + 2833X^2 + 3090X + 4382) \% 255$$

ここで、A%Bは、AをBで割った際の余りを表す。

【0079】

【発明の効果】以上説明したように、本発明によれば、パスワードを含む秘密情報、利用者の氏名を含む公開情報および文書の文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置したり、受信文書から配置された印鑑イメージを取り出して照合したりする構成を採用しているため、印鑑の不正使用を防止できると共に、検印後の文書の改変を検出できる。

【図面の簡単な説明】

【図1】本発明のシステム構成図である。

【図2】本発明の概念説明図（その1）である。

【図3】本発明の概念説明図（その2）である。

【図4】本発明の動作説明フローチャート（その1）である。

【図5】本発明の画面例である。

【図6】本発明の動作説明フローチャート（その2）である。

【図7】本発明の画面例である。

【図8】本発明の動作説明フローチャート（その3）である。

【図9】本発明の動作説明フローチャート（その4）である。

【図10】本発明の画面例である。

【図11】本発明の印鑑イメージテーブル例である。

【図12】本発明のキーワード組み込み説明図である。

【符号の説明】

1：クライアント

2：入出力手段

3：配置手段

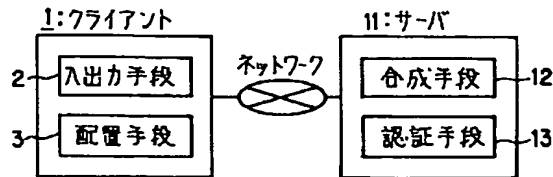
11：サーバ

12：合成手段

13：認証手段

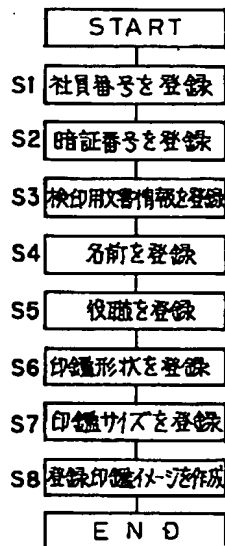
【図1】

本発明のシステム構成図



【図4】

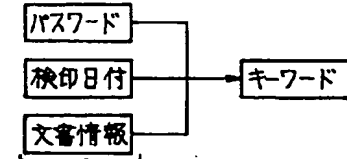
本発明の動作説明フローチャート（その1）



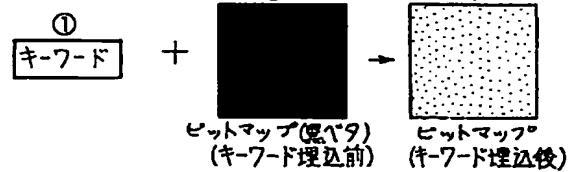
【図2】

本発明の概念説明図（その1）

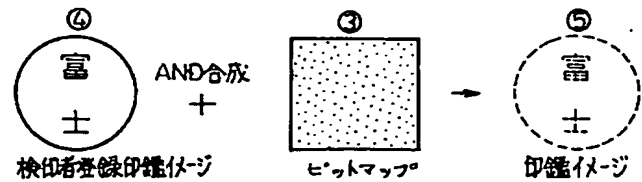
(a) ビットマップ（識別データ）の作成手順  
(a-1)



(a-2)

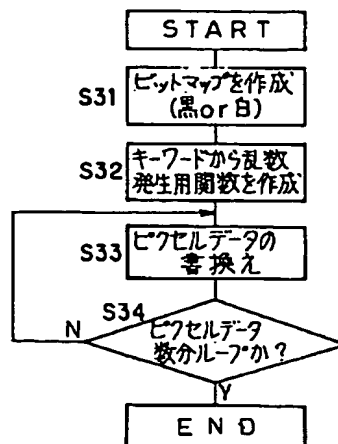


(b) 検印用印鑑イメージの作成手順



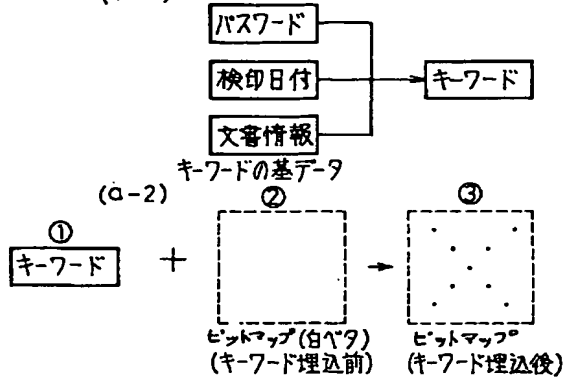
【図8】

本発明の動作説明フローチャート（その3）

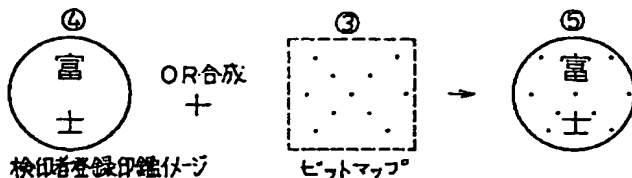


【図3】

## 本発明の概念説明図(その2)

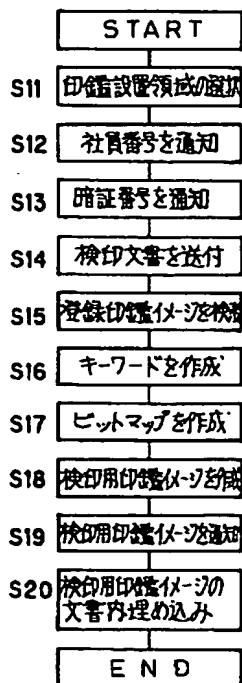
(a) ビットマップ(識別データ)の作成手順  
(a-1)

(b) 検印用印鑑イメージの作成手順



【図6】

## 本発明の動作説明フローチャート(その2)



【図5】

## 本発明の画面例

(a)

検印者情報の設定

社員番号: 1234567890

暗証番号: \*\*\*\*\*

検印用文書情報

☒ 文書内文字数 ☐ 特定文字の文字数(複数可)

☐ ひらがな文字数 ☐ カタカナ文字数

☐ 空白文字数 ☐ 数字文字数

垂投書

登録 取消

検印者情報の設定画面

(b)

印鑑イメージの登録

名前: 富士 役職: 開発部長

印鑑形状: 丸(日付付有) ↓

印鑑サイズ: 12 mm

登録 取消

開発課長  
98 03 03  
富士

印鑑イメージの登録画面

【図11】

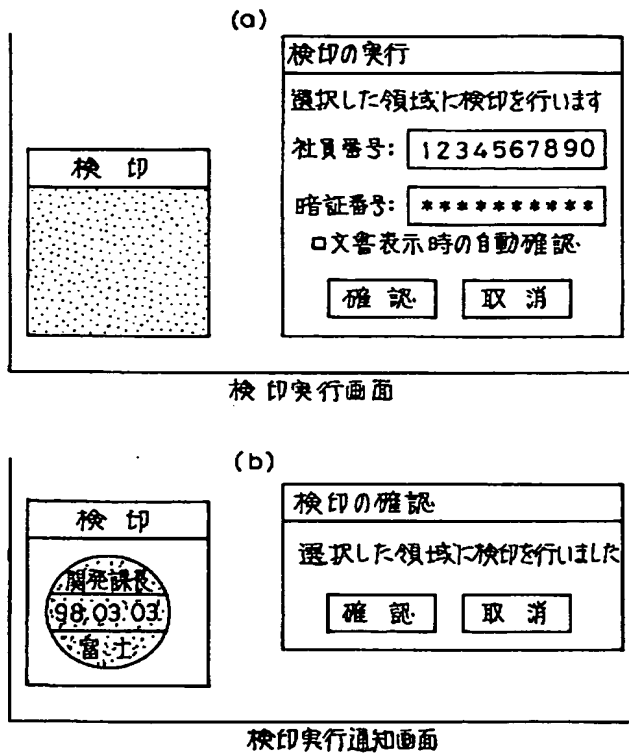
## 本発明の印鑑イメージテーブル例

印鑑イメージテーブル

社員番号	パスワード	イメージファイル
00001	XXXXXX	印鑑イメージ

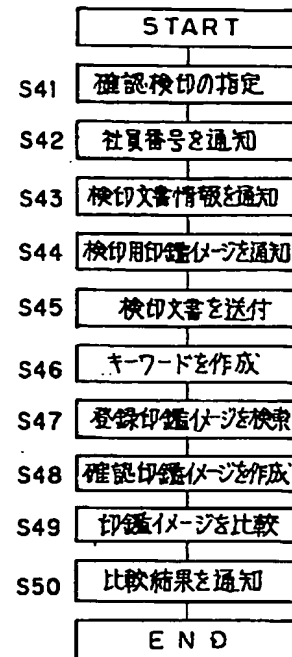
【図 7】

本発明の画面例



【図 9】

本発明の動作説明フローチャート(その4)



【図 12】

本発明のキーワード組み込み説明図

- (a)パレットデータ
- |       |       |       |       |       |       |       |     |
|-------|-------|-------|-------|-------|-------|-------|-----|
| 黒     | グレー-1 | グレー-2 | グレー-3 | グレー-4 | グレー-5 | グレー-6 | ... |
| Index | 0     | 1     | 2     | 3     | 4     | 5     | 6   |
- (b)ビツヘルデータ
- |        |        |        |        |        |        |        |     |
|--------|--------|--------|--------|--------|--------|--------|-----|
| Index0 | Index0 | Index0 | Index0 | Index0 | Index0 | Index0 | ... |
|--------|--------|--------|--------|--------|--------|--------|-----|
- (c)パスワードを「1234」  
 検印日付を「980303」  
 文書内文字数を「980302」
- (d)キーワード「1234980303980302」を作成
- (e)キーワードを4分割し、定数「1900」「2833」「3090」「4382」
- (f)三次曲線を作成
- $$Y = 1900X^3 + 2833X^2 + 3090X + 4382$$
- (g)  $Y = (1900X^3 + 2833X^2 + 3090X + 4382) \% 256$   
 注)  $A \% B \rightarrow A$ を $B$ で割った際の余り

【図10】

本発明の画面例

